

REMARKS

Applicant wishes to thank Examiner Pyzochoa for the courtesy of an interview on December 18, 2007. The Examiner indicated that the rejection of Claims 15-21, 24, 25, 28, 29, 33, and 34 under 35 U.S.C. § 102(e) being anticipated by *Tsukahara et al.* (U.S. 6,920,222) was a clerical error and that it is withdrawn. The Examiner also further explained the motivation for combining the *Darshan* and *Tehranchi* reference with the *Tsukahara* reference. Claims 1-21, 26-29 and 31-35 remain in the application.

The Office Action rejected Claim 35 under 35 U.S.C. § 112 as being indefinite. Applicant has amended Claim 35 to overcome the rejection and respectfully requests that the rejection be withdrawn.

The present invention is directed towards efficient processing and decryption of scrambled video data to allow a user to fast forward and decrypt the scrambled video without suffering performance issues. (Pg. 28, lns. 1 – 4). It accomplishes this by using storage information with all of the list of the descrambling keys embedded. (Pg. 27, lns. 21 – 25) It can also selectively choose to decrypt and display only certain frames. For example, it can choose to only decrypt and display I pictures (intraframe-coded picture) when fast forwarding because only I pictures can be drawn and displayed based solely on the data that it contains. Thus, B pictures (bidirectional frame) and P pictures (predictive pictures) are not selected to be decrypted or displayed when fast-forwarding. (Pg. 49, lns. 3 – 8; Fig. 14).

The Office Action rejected Claims 1-8, 11-14, 26, 27, 31, 32, and 35 under 35 U.S.C. § 103(a) as being unpatentable over *Tsukahara* in view of *Darshan* (U.S. 7,106,749) and further in view of *Teharanchi* (U.S. 7,242,772).

Neither *Tsukahara*, *Darshan*, nor *Teharnchi* teach or suggest “storage means for storing . . . the storage information” wherein “the storage information includes a list of the descrambling keys which includes all of the descrambling keys.”

Tsukahara is directed towards allowing non-paying or unauthorized viewers of a pay-per-view program to watch parts of a pay-per-view or subscription program for a period of time in order to increase their propensity to subsequently order the pay-per-view program. (Abstract; Col. 2, lns. 61 – 67) It uses a partial viewing authorization information in conjunction with subscriber contract information to determine whether a user can partially watch the pay-per-view program. (Col. 6, lns. 54 – 58)

In *Tsukahara*, ECM analyzer 32 decrypts the ECM using the work keys to retrieve the scrambling keys. *Tsukahara*, however, does not disclose that the ECM analyzer 32 extracts a list of descrambling keys. *Tsukahara* only extracts the descrambling keys and not a list of descrambling keys. Since *Tsukahara* only extracts the descrambling keys and not the list of descrambling keys, it does not store the list of descrambling keys. This is especially true considering that *Tsukahara* does not provide any structure to store the list of descrambling keys.

Darshan seeks to improve the playback performance of a scrambled content by using an index built during playback of the scrambled content. Thus when a trick mode is performed, a trick mode parameter is determined based at least in part on the index built when the scrambled content is first played. The trick mode parameter may comprise any suitable parameter useful in performing a trick mode and typically comprises an indication of a location in at least partially scrambled data stream at which descrambling and playback are to begin or to continue. (Abstract; Col. 8, ln. 57 – Col. 9, ln. 12)

Darshan discloses receiving scrambled packets, but does not disclose receiving a list of descrambling keys. Thus, *Darshan* also does not teach storing the list of descrambling keys.

Tehranchi is directed towards an apparatus and a method for encrypting a data stream as plurality of sequential data blocks, each block having an assigned encryption key and for providing a secure method for synchronizing each encryption key with a corresponding data block. (Col. 5, Ins. 15 – 20).

Tehranchi teaches that the data origination site 12 and the data destination site 14 should have a key and synchronization generator 28 and 40 respectively, but does not teach that there should be any structure to store the list of descrambling keys. (Fig. 1) Key and synchronization generator 28 provides encryption engine 22 with an encryption key 50 for each data block 26 as shown in Figures 2 and 4 and transmits the encryption keys 50 to destination key and synchronization generator 40 through key transmission channel 34. It also generates a synchronization index that associates each generated encryption key 50 with its corresponding data block 26 and transmits the information to key and synchronization generator 40 through block synchronization channel 78. (Col. 7, Ins. 40 – 52; Fig. 1) Destination key and synchronization generator 40 receives input data from key transmission channel 34 and block synchronization channel 78 and as output, provides the necessary encryption key and synchronization data for decryption engine 38. (Co. 8, Ins. 42 – 62). However, *Tehranchi* does not disclose a structure of a storage means for storing the list of descrambling keys.

Furthermore, as seen in Figure 1, destination site storage buffer 36 only stores the ciphertext data stream from encryption engine 22 and there is no indication hat it stores the list of descrambling keys. (Col. 8, Ins. 46 – 49). In fact, destination site storage buffer 36 does not receive information from decryption engine 38 which contains key and synchronization

generator 40 at all, but instead only transmits the ciphertext data stream to decryption engine 38 as indicated by the unidirectional arrow from destination site storage buffer 36 to decryption engine 38. (Fig. 1).

In contrast, in the present invention, the scramble key list which shows the scramble key associated with the TS packets, as seen in Figure 7, is stored in the scrambling key list holding unit 203 as seen in Figure 1. (Pg. 42, lns. 20 – 22). Descrambling unit 211 descrambles one TS packet passed from the TS packet extracting unit 210 using the scrambling key extracted by the scrambling key list interpretation unit 212 from the scrambling key list holding unit 203. (Pg. 48, lns. 13 - 24; Figs. 1, 8).

Neither *Tsukahara*, *Darshan*, nor *Tehranchi* disclose wherein “in the particular reproduction mode, said list extraction means extracts all descrambling keys from the list of descrambling keys.” The Office Action cites to Column 10, lines 26 – 64 in *Tsukahara* for the feature of the present invention. However, *Tsukahara* only discloses using descrambling keys to descramble the data stream based on the authorization of the subscriber contract information. It does not disclose extracting the descrambling keys from the list of descrambling keys for a particular reproduction mode. That is, *Tsukahara* does not disclose the use of a list of descrambling keys and therefore does not extract the descrambling keys from the list of descrambling keys.

Darshan does not disclose the use of descrambling keys from the list of descrambling keys, but rather only teaches the use of a trick mode. *Darshan* does not use a list of descrambling keys.

Tehranchi also does not teach the features of the present invention. *Tehranchi* only teaches key and synchronization generator 40 in destination site 14 receives the encryption keys

50 and synchronization index from key and synchronization generator 28 in data origination site 12. (Col. 8, lns. 58 – 62) Thus, key and synchronization generator 40 does not extract the encryption keys 50 from the synchronization index but rather receives encryption key 50 from key and synchronization generator 28.

In contrast, in the present invention, ECM interpretation unit 301 extract the scrambling key list from the storage ECM stored in the HDD 202. (Pg. 47, lns. 9 – 11, Fig. 1). The scrambling key list is stored in scrambling key list holding unit 203. (Pg. 47, lns. 12 – 14, Fig. 1). Scrambling key list interpretation unit 212 of the descrambling process unit 204 then extracts the scrambling keys from the scrambling key list stored in scrambling key list holding unit 203. (Pg. 48, lns. 14 – 18; Figs. 1, 4). Thus, in the present invention, the scrambling keys are extracted from the scrambling key list and the scrambling keys are not nakedly received from the broadcast apparatus 100.

Furthermore, the Office Action admits that *Tsukahara* fails to disclose the use of a particular reproduction mode wherein “the particular reproduction mode is a mode which includes a fast-play mode and in which only predetermined frames selectively extracted from less than all of the frames are descrambled and reproduced.” The Office Action states that it would have been obvious to a person of ordinary skill in the art to implement *Tsukahara*’s inhibit viewing mode as a fast forward mode using the trick mode taught in *Darshan*. *Tsukahara* is designed to allow previews of pay-per-view programs. Such pay-per-view programs are often broadcast uniformly and contemporaneously to users with the ability of the users to watch the program determined by the subscriber information. If, *Darshan* is combined with *Tsukahara*, the inhibit viewing mode would be fast forwarded. That is, the user would skip through the inhibit viewing portion of the pay-per-view program. Thus, the broadcast apparatus would have to

broadcast the pay-per-view program at different times to different people. This would require significantly more energy and resources to individualize the broadcast schedule.

Also, if the inhibit viewing mode is fast forwarded, then users may not have a chance to subscribe to the pay-per-view program. Hypothetically if a user wanted to watch a pay-per-view program after viewing the preview portion, the user would have to call the cable company or attempt to subscribe to the pay-per-view program. If, however, the pay-per-view has reached the inhibit viewing portion of the pay-per-view program before the user has successfully subscribed to the pay-per-view program and the inhibit viewing portion is fast-forwarded, then the user would be missing much of the pay-per-view program while he is attempting to subscribe to the pay-per-view program. This would be a strong disincentive for the user to subscribe to the pay-per-view program and render *Tsukahara* generally inoperable for its intended purpose.

Furthermore, even if the combination of *Tsukahara* and *Darshan* were combined to produce a DVR that could record the program and then allow fast-play of the recorded program, and there is no suggestion in either reference that such a hypothetical combination should be made, the hypothetical combination would still render the combination generally inoperable for the intended purpose of *Tsukahara*. Notably, in order to fast forward through the program, the user would still have to wait for the initial broadcast in the inhibit viewing mode before watching the program since the DVR only records what is broadcasted. This lag would be prohibitive, especially in pay-per-view programs in which live viewing is essential, such as in sports or in pay-per-view programs which the user has already partially seen and wants to watch only a portion of the program such as a movie.

[I]t is generally settled that the change in prior art device which makes the device inoperable for its intended purpose cannot be considered to be an obvious change.

Hughes Aircraft Co. v. United States, 215 U.S.P.Q. 787, (Ct.Cl. Trial Div. 1982)

Thus, it would not be obvious to a person having ordinary skill in the art to implement *Tsukahra's* inhibit viewing mode as a fast forward mode.

With respect to Claims 12, 26, 27, 31, and 32 all arguments for patentability with respect to Claim 1 are repeated and incorporated herein.

The Office Action admits that *Tsukahara* fails to disclose that “the reception means sequentially receives a TS packet including (a) the predetermined unit of scrambled content, and (b) auxiliary information including a descrambling key and information for associating the descrambling key with scrambled content” in Claim 13.

However, *Tehranchi* also fails to disclose that “the reception means sequentially receives a TS packet including (a) the predetermined unit of scrambled content, and (b) auxiliary information including a descrambling key and information for associating the descrambling key with scrambled content.” In *Tehranchi*, the frames, the encryption keys 50, and the synchronization index are transmitted separately. Thus, there is no indication that the auxiliary information is attached to a TS packet itself.

In contrast, in one embodiment of the present invention, the broadcast apparatus 800 in Figure 27 does not generate a scrambling key list. Instead, the broadcast apparatus 800 adds auxiliary information including identifying information on the scrambled content to the normal reproduction ECM, such as packet numbers so as to help the reception apparatus 900 to generate a scrambling key list and scrambling keys, and broadcasts it to the reception apparatus 900. (Pg. 66, Ins. 7 – 15). The security module 1000, which is set and integrated with the reception apparatus 900 receives the normal reproduction ECM and the scrambled content, stores the

scrambled content while generating a scrambling key list based on the auxiliary information added to the normal reproduction ECM. (Pg. 66, lns. 16 – 23).

The Office Action rejected Claim 10 under 35 U.S.C. §103(a) as being unpatentable in view of *Tsukahara*, *Darshan*, *Tehranchi*, and *Ando* (U.S. Patent App. No. 2003/0133699).

Ando is directed to a recording/playback system to record video from a digital video datastream and store it for later playback. (Abstract; ¶ 0001).

The Office Action admitted that *Tsukahara*, *Darshan*, and *Tehranchi* do not disclose “I picture judgment means for judging whether the extracted predetermined unit of scrambled content consists of a portion of an I picture/an I picture or not, based on the extracted I picture information.”

Ando, however, also does not disclose “I picture judgment means for judging whether the extracted predetermined unit of scrambled content consists of a portion of an I picture/an I picture or not, based on the extracted I picture information.” *Ando* only discloses that the I pictures is located at the head of each set of TS packet and to search for an I pictures address. Thus, the invention only needs to look at the head of each set of TS packets to discover the I picture. There is no need to analyze embedded information to determine if a packet is an I picture or not since a predetermined location of a TS packet is guaranteed to be an I packet. Thus, there is no indication that *Ando* teaches using the extracted I picture information to determine whether the extracted predetermined unit of scrambled content is a portion of an I picture/an I picture, or not.

In contrast, in the present invention, the broadcast apparatus embeds the information indicative of an I picture in the unscrambled portion in the TS packet. The reception apparatus then makes a judgment of whether the extracted predetermined unit of scrambled content is a

portion of an I picture/an I picture, or not based on the embedded information. (Pg. 50, ln. 19 – Pg. 51, ln. 6).

The Office Action rejected Claims 15-21, 28, 29, 33, and 34 under 35 U.S.C. § 103(a) as being unpatentable over *Tuskahara* in view of *Tehranchi* (U.S. 7,242,772).

The Office Action admits that *Tuskahara* fails to disclose “attaching means for attaching auxiliary information, which is used to generate a list of the descrambling keys, wherein the auxiliary information includes (a) information for identifying each of the frames and (b) each of the descrambling keys selected for the frame” in Claim 15.

However, *Tehranchi* also fails to disclose “attaching means for attaching auxiliary information, which is used to generate a list of the descrambling keys, wherein the auxiliary information includes (a) information for identifying each of the frames and (b) each of the descrambling keys selected for the frame.” In *Tehranchi*, the frames, the encryption keys 50, and the synchronization index are transmitted separately. Thus, there is no indication that the auxiliary information is attached to the frame itself.

In contrast, in one embodiment of the present invention, the broadcast apparatus 800 in Figure 27 does not generate a scrambling key list. Instead, the broadcast apparatus 800 adds auxiliary information including identifying information on the scrambled content to the normal reproduction ECM, such as packet numbers so as to help the reception apparatus 900 to generate a scrambling key list and scrambling keys, and broadcasts it to the reception apparatus 900. (Pg. 66, lns. 7 – 15). The security module 1000, which is set and integrated with the reception apparatus 900 receives the normal reproduction ECM and the scrambled content, stores the scrambled content while generating a scrambling key list based on the auxiliary information added to the normal reproduction ECM. (Pg. 66, lns. 16 – 23).

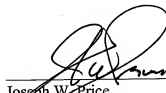
All arguments for patentability with respect to Claim 1 are repeated and incorporated herein for Claims 17, 31, and 32.

Claims 2-11, 13-14, 16, and 18-21, and 35 depend from and further define Claims 1, 12, 15, and 17 and are patentable for at least the reasons given.

If the Examiner believes that a telephone interview will help further the prosecution of this case, the undersigned attorney can be contacted at the listed telephone number.

Very truly yours,

SNELL & WILMER L.L.P.

A handwritten signature in black ink, appearing to read 'J. W. Price', is written over a horizontal line.

Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799